Polarisation Encryption/Decryption Module

Glückstad, Jesper; Mogensen, Paul Christian

Publication date:
2002

Document Version
Publisher's PDF, also known as Version of record

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23794 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/DK01/00598

(22) International Filing Date:
14 September 2001 (14.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/232,429 14 September 2000 (14.09.2000) US
PA 2000 01367 14 September 2000 (14.09.2000) DK

(71) Applicant *(for all designated States except US)*: **FORSKNINGSCENTER RISOE** [DK/DK]; P.O. Box 49, Frederiksborgevej 399, DK-4000 Roskilde (DK).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GLÜCKSTAD, Jesper** [DK/DK]; Voldumvej 45, St. tv, DK-2610 Rødovre (DK). **MOGENSEN, Paul, Christian** [GB/DK]; Sandbygårdsvej 34, st. tv, DK-2700 Brønshøj (DK).

(74) Agent: **PLOUGMANN & VINGTOFT A/S**; Sankt Annæ Plads 11, P.O. Box 3007, DK-1021 Copenhagen K (DK).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

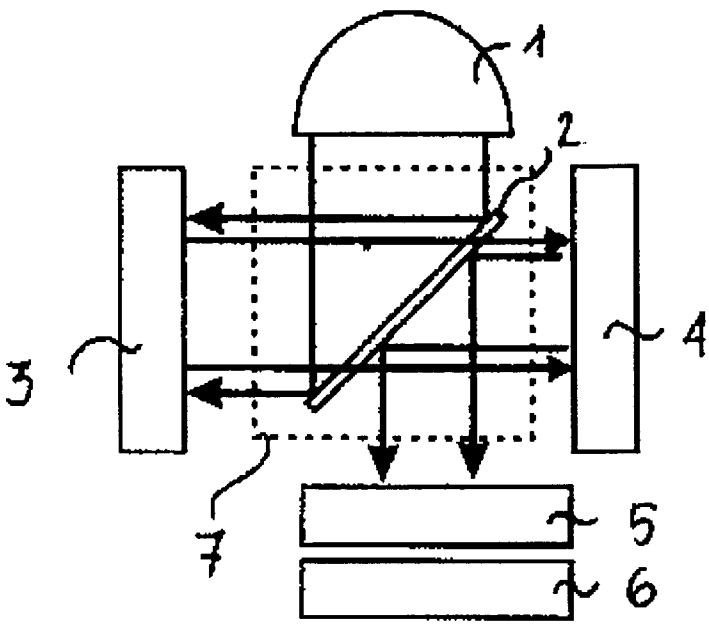
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: POLARISATION ENCRYPTION/DECRYPTION MODULE



(57) Abstract: A polarisation encryption/decryption module comprising at least two array based modulating devices, preferably spatial light modulators (SLMs), at least one array based intensity detector, and at least one source of electromagnetic radiation. A local region of information displayed on a first of the modulating devices has corresponding local regions on each of the other modulating devices and on each of the detectors. Preferably uses XOR operations. The module is compact in size and capable of performing encryption as well as decryption. Provides fast encryption/decryption because the key may be changed rapidly. May be used for real time encryption/decryption of motion pictures. Further, a method of polarisation encrypting and decrypting information. The encryption/decryption is performed optically while the communication is performed electronically.

WO 02/23794 A2

POLARISATION ENCRYPTION/DECRYPTION MODULE

TECHNICAL FIELD

The present invention relates to an encryption/decryption module for encrypting/decrypting information. More specifically the invention relates to a polarisation encryption/decryption module for optically encrypting/decrypting information.

The invention also relates to the possibility of securing data transmission over the internet or local area networks (LANs) by optical encryption.

BACKGROUND OF THE INVENTION

The current encryption processes used for securing data transmission are based on the electronic scrambling of the information transmitted and as such there is a trade off between security and transmission speed. The use of a long (more secure) key inherently slows the data transmission rate due to the serial nature of the scrambling process and shorter keys (less than 128 bits) have already been shown to be relatively simple to compromise. It is therefore an object of the present invention to find a method and apparatus using optical encryption to scramble and hence secure information prior to electronic transmission since the encryption speed is independent of the key size, with the use of a 1000 bit key being no slower than the use of a 50 bit key.

The recent expansions in the internet and data-communications traffic has raised questions regarding the optimum approach for the secure transfer of sensitive information. There is thus currently a considerable level of interest in the application of optical techniques to the encryption of data for the secure transmission and storage of information. The high space-bandwidth product and the difficulty of unauthorised access, copying and falsification have therefore been cited as reasons why an optical approach to encryption may be advantageous. Current state of the art encryption processes used for securing data transmission are based on the electronic scrambling of information. Therefore, a practical method using optical encryption to scramble and hence secure information prior to electronic transmission may be advantageous, because the encryption speed in an optical system is essentially independent of the key size, due to the inherently parallel nature of the operation.

The development of optical encryption schemes has been the subject of much effort in recent years with the majority of the proposed schemes focusing on the decryption of information stored in a fixed element. The double phase-key encoding scheme, in which image plane and Fourier plane phase keys scramble amplitude information represents the earliest work. Recent approaches have included, among others, the application of XOR operations for encryption, the inclusion of biometrics, the use of photo-refractive materials and the application of the generalised phase contrast technique. These techniques have been successfully applied using fixed keys and input information, however a system for optical encryption at the high data rates puts different requirements on the type of approach that can be used. Digital holography and phase shifting interferometry (PSI) have been proposed as methods for optically encrypting information for data transmission. In these systems, the information to be encoded is displayed and encrypted optically and the encrypted information is captured and stored electronically for transmission via conventional means. The PSI system has been successfully demonstrated, but requires the generation of four phase shifted versions of a given frame in order to obtain the amplitude and phase information to reconstruct the information completely in the decrypting system, representing a somewhat inefficient use of the available bandwidth. The information capacities of systems based on digital holography are largely limited by the current resolutions of the CCD cameras and spatial light modulators (SLM) used to record and regenerate the encrypted optical holograms. Both these techniques require significant electronic processing of the information before transmission, which may limit their suitability for application in high speed systems.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide an encryption/decryption module which is compact in size and fast, and which is capable of performing encryption as well as decryption. It is a further object of the present invention to provide a method of performing encryption/decryption using such a module. It is an even further object of the present invention to provide a method for transmitting information in a safe manner without reducing the speed of transmission at which no encryption or decryption takes place.

Thus, according to the present invention there is provided a polarisation encryption/decryption module comprising

- at least two array based modulating devices,
- at least one array based intensity detecting device,
- at least one source of electromagnetic radiation,

the at least two array based modulating devices having substantially the same functionality,

the at least one source(s) of electromagnetic radiation being capable of emitting electromagnetic radiation,

a first of the array based modulating devices being capable of receiving and modulating electromagnetic radiation which has been emitted from the at least one source(s) of electromagnetic radiation and of displaying information to be encrypted/decrypted,

a second of the array based modulating devices being capable of changing the spatial polarisation state of the electromagnetic radiation, so as to perform an operation of encrypting/decrypting the information displayed at said first array based modulating device,

wherein a local region of information displayed on said first array based modulating device has corresponding local regions on each of the other of the at least two array based modulating devices and on each of the at least one array based intensity detecting device(s).

The source(s) of electromagnetic radiation may comprise one or more lasers, one or more masers, one or more white "cold" sources (such as a white tungsten-halogen "cold" source) and/or any other suitable kind of source being capable of emitting electromagnetic radiation, even an ordinary light bulb.

The at least two array based modulating devices having substantially the same functionality means that they are capable of performing modulating operations in a substantially identical manner. They may be identical devices, but there may also be minor differences, such as one may be a reflective device while another one is a transmissive device, as long as the modulating operations performed by the different

devices are substantially identical. Even more substantial differences may be present between the modulating devices, as long as these differences do not influence the modulating operations. Thus, one or more of the modulating devices may additionally be capable of performing other kinds of operations, such as emitting electromagnetic radiation, while other of the modulating devices may not be capable of performing such operations. Even though the functionality in a broad sense of the devices in this case can not be considered to be substantially the same, it will still be regarded as such in the present context since the extra functionality of the one modulating device does not influence the modulating operations.

The information to be encrypted/decrypted may be electronic data which needs to be sent in a secure manner from one computer device to another via a global or local computer network. The term "secure manner" should be interpreted as meaning in such a manner that the information can not be readily retrieved in case a "non-rightful" person (i.e. a person for who the information is not intended) accidentally or via a criminal or deceitful act gains access to the information being sent. Such electronic data may be in the form of one or more images (e.g. one picture or a sequence of pictures, such as a motion picture), documents (e.g. confidential text documents), musical files (e.g. MP3 files) and/or any other suitable kind of data.

The term "a local region of information" is to be interpreted as meaning a spatially localised part of the information. In case the information is arranged in a two-dimensional array a "local region" is an area of said two-dimensional array. The region may be a single pixel or a number of pixels being adjacent to one another (such as a 2x2 or 4x4 pixel array). If the local region of the first modulating device is a single pixel the local regions of the other devices are not necessarily a single pixel too. They may contain more pixels as long as these pixels are positioned adjacent to each other.

At least one of the at least two array based modulating devices may be a dynamic array based modulating device. Preferably, at least one of the modulating devices comprises a two-dimensional array, but alternatively or additionally at least one of them may comprise a one-dimensional array. Alternatively or additionally, at least one of the at least two array based modulating devices may be a fixed array based modulating device.

Furthermore, at least one of the at least two array based modulating devices may be a reflective optical device, e.g. comprising a mirror, in which case the electromagnetic radiation incident on that modulating device will be reflected from it. Alternatively or additionally, at least one of the at least two array based modulating devices is a transmissive optical device, so that the electromagnetic radiation incident on that modulating device will be transmitted through it. This will be described in further detail elsewhere in the present application.

In case at least one of the array based modulating devices is a reflective optical device, such a modulating device may be a reconfigurable spatial light modulator (SLM). In this case it comprises a two-dimensional array.

At least one of the at least one electromagnetic source(s) may be incorporated in one of the at least two array based modulating devices. In this case electromagnetic radiation may be emitted via that modulating device. The modulating device in question is preferably a transmissive optical device, in which case the source is positioned at the back part of the modulating device, emitting electromagnetic radiation towards the modulating device. The radiation passes through the modulating device, and during this passage the radiation is modulated by the modulating device.

Preferably, at least one of the at least two array based modulating devices is capable of modulating the ellipticity of the electromagnetic radiation, such as modulating the linear polarisation state of the electromagnetic radiation or the circularity of the polarisation of the electromagnetic radiation.

Preferably, at least one of the at least two array based modulating devices is a ferro-electric liquid crystal spatial light modulator (FLC-SLM). Such devices have the advantage of being commercially available, compact in size, relatively cheap and fast. It is therefore possible to provide an encryption/decryption module which is cheap and fast when applying such modulating devices.

Alternatively or additionally, at least one of the at least two array based modulating devices may be based on a birefringent material or effect and/or it may be based on an anisotropic refractive index effect, such as astigmatism, and/or it may be a nematic liquid

crystal spatial light modulator (SLM), and/or it may be based on arrays of polarising elements.

As mentioned above the information to be encrypted/decrypted may comprise at least one two-dimensional image, such as a picture or a sequence of pictures, such as a motion picture or part of a motion picture. Alternatively or additionally, it may comprise at least one one-dimensional array of information, such as a string of data.

Preferably, the outer dimensions of the module do not exceed 100 mm x 100 mm x 100 mm, such as they do not exceed 80 mm x 80 mm x 50 mm, such as they do not exceed 75 mm x 75 mm x 30 mm. The module is thus preferably small enough to be directly inserted in a PC or to be positioned on an ordinary desktop without occupying an excessive amount of space. It is thus possible for "private persons" to use the module in connection with a PC positioned in the home of the person.

At least one of the at least one source(s) of electromagnetic radiation may be capable of emitting electromagnetic radiation within the optical frequency range of the electromagnetic spectrum, i.e. it is capable of emitting ordinary light. Alternatively or additionally at least one of the sources may be capable of emitting electromagnetic radiation within other ranges of the electromagnetic spectrum, such as the infrared range, the ultraviolet range, the microwave range or any other suitable range. The source(s) may be capable of emitting electromagnetic radiation containing a continuous range of wavelengths (such as in the case of a ordinary light bulb) or it/they may only be capable of emitting electromagnetic radiation of a single wavelength (such as in the case of a laser).

At least one of the at least one source(s) of electromagnetic radiation may be a laser, such as a diode laser, a HeNe laser or any other suitable kind of laser. Alternatively or additionally, at least one of the at least one source(s) of electromagnetic radiation may be any other suitable kind of source as has already been described above. A diode laser is very preferred since it may have very small dimensions. Thus, the overall dimensions of the module may be reduced by using a diode laser instead of a source having larger dimensions. However, other kinds of sources may be chosen due to other properties, such as the desired wavelength or range of wavelengths, heat productions etc.

At least one of the at least one array based intensity detecting device(s) may preferably be a charge coupled device (CCD) camera. Alternatively or additionally, at least one of the at least one array based intensity detecting device(s) may be a dedicated complementary metal oxide semiconductor (CMOS) detector.

The present invention further provides a method of polarisation encrypting/decrypting information using a module as described above, the method comprising the steps of

a) at least one of the at least one source(s) of electromagnetic radiation emitting electromagnetic radiation,

b) a first of the at least two array based modulating devices receiving and modulating electromagnetic radiation which has been emitted from the at least one source(s) of electromagnetic radiation,

c) the first of the at least two array based modulating devices displaying the information to be encrypted/decrypted,

d) a second of the at least two array based modulating devices changing the spatial polarisation of the electromagnetic radiation, thereby performing an operation of encrypting/decrypting the information displayed at said first array based modulating device,

e) at least one of the at least one array based intensity detecting device(s) detecting the result of the encryption/decryption process performed by said second array based modulating device,

the encryption/decryption being performed in such a way that a local region of information displayed on said first array based modulating device has corresponding local regions on each of the other of the at least two array based modulating devices and on each of the at least one array based intensity detecting device(s).

This has already been described.

In one embodiment the steps a)-e) may be performed two or more times. Thus, in the encryption case, information which has already been encrypted once may be subject to the above mentioned method at least once more. The data will thereby become even more scrambled, and the original information will become even more difficult to retrieve by "non-rightful" persons as defined above. It may be possible to choose the number of times the steps a)-e) should be performed in a particular case. That is, in case the data to be sent is very sensitive a large number of times can be chosen, and in case the data is less sensitive a smaller number of times, maybe just once, can be chosen. Alternatively, the number of times may be fixed in advance for a given module. In the decryption case the number of times will be determined by the number of times which was used when the information was encrypted, since the decryption method must be performed once for each time the information was encrypted.

In case at least one of the at least one source(s) of electromagnetic radiation is incorporated in one of the at least two array based modulating devices, step a) may comprise emitting electromagnetic radiation via the one of the at least two array based modulating devices having the electromagnetic source(s) incorporated in it. This has already been described above.

Step d) may be performed by modulating the ellipticity of the electromagnetic radiation or by modulating the linear polarisation state of the electromagnetic radiation or by modulating the circularity of the electromagnetic radiation or by changing the spatial polarisation of the electromagnetic radiation in any other suitable way.

In case the information to be encrypted/decrypted comprises two or more successive two-dimensional images, the steps a)-e) may be performed at least once for each two-dimensional image, and step d) may be performed in a way which is different for each image, so that a sequence of encrypted/decrypted images is produced. In this case each image is encrypted/decrypted individually by performing the steps a)-e) at least once for each image. By performing step d) differently for each image a different encryption/decryption key is effectively used for each image. This is only possible when using a fast and dynamic system in which the key (in this case the way in which the spatial polarisation of the electromagnetic radiation is changed) may be exchanged rapidly, so as to not slow down the encryption/decryption process when doing so. The fact that it is possible to exchange the key on an image to image basis provides a very secure

system, since it is necessary to obtain a separate key for each image in order to gain access to the information. So even though a "non-rightful" person obtains one key, he or she will only gain access to the corresponding image, i.e. he or she will not gain access to the complete information. Gaining access to just one image may not make the person capable of making sense of the information, the information thus effectively still being protected. This approach may e.g. be useful in case the information is a motion picture or part of a motion picture. Thus, the present invention is very useful for controlling the distribution of motion pictures etc., e.g. the distribution of motion pictures via a global computer network or via a cable network. The invention may, e.g., be used for controlling that only persons who have paid the prescribed fee, etc., may gain access to the motion picture. The invention may, thus, advantageously be used in combination with a subscriber or 'pay-per-view' system for distribution of motion pictures.

The present invention further provides a method of polarisation encrypting and decrypting information using at least two polarisation encryption/decryption modules as described above, the method comprising the steps of

- a first of the at least two polarisation encryption/decryption modules encrypting the information using a method as described above,
- transmitting the encrypted information from said first polarisation encryption/decryption module to a second of said at least two polarisation encryption/decryption modules,
- said second polarisation encryption/decryption module decrypting the information using a method as described above.

The at least two modules should be at least substantially identical. All of them should be capable of encrypting as well as decrypting information. This provides a simple system where only one module is needed in order to perform encryption as well as decryption. It is therefore possible to perform two-way communication with the users involved having only one module each. Thereby a flexible system is provided without being too space consuming (since different modules for encryption and decryption, respectively, would require the presence of at least two modules per user).

At least the transmitting step may be performed using at least one computer device. Each of the modules is preferably inserted into or embedded in a computer device, such as a personal computer (PC). The transmission preferably takes place via a computer network,

either a global computer network, such as the internet or a world area network (WAN), or a local computer network, such as a local area network (LAN) or an intranet. The computers involved should in this case be at least temporarily connected to the computer network. Alternatively, the two computers involved may be directly connected to each other.

The method may be performed using a plurality of polarisation encryption/decryption modules as described above, in which case the method further comprises the steps of

- transmitting the encrypted information from said first polarisation encryption/decryption module to at least a third of said plurality of polarisation encryption/decryption modules,
- each of said at least third polarisation encryption/decryption module(s) decrypting the information using a method of decryption as described above.

In this case the first module may transmit the encrypted information at least substantially simultaneously to a number of recipients. Each of these recipients may subsequently decrypt the information independently of each other. This may e.g. be useful in case the sender is a distributor providing information to a number of recipients, e.g. on a subscription basis. Such a distributor may be interested in distributing the same material/information to all the customers or to a certain group of subscribers. In order to ensure that only paying subscribers receive the information the distributor may choose to transmit the information in an encrypted form.

BRIEF DESCRIPTION OF THE DRAWINGS

Reference will now be made to the accompanying drawings in which

Fig. 1 shows a reflection geometry set-up of a polarisation encryption/decryption module according to the invention,

Fig. 2 shows a transmission geometry set-up of a polarisation encryption/decryption module according to the invention,

Fig. 3 shows a preferred embodiment of a polarisation encryption/decryption module according to the invention,

Fig. 4 shows a schematic representation of an encryption/decryption method according to the invention,

Fig. 5 shows a schematic view of the encryption, transmission and decryption of a sequence of images,

Fig. 6 shows the optical configuration for a dual FLC-SLM encryption/decryption system,

Fig. 7 shows a simulation result for a 256x256 decryption of (a) the encrypted information by an XOR operation with (b) the key to reveal (c) the original information, and

Fig. 8 shows experimental results showing (a) the successfully decrypted information and for comparison (b) the original image displayed on SLM 1 and imaged directly onto the CCD.

DETAILED DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a generic reflection geometry set-up. The module comprises a source of electromagnetic radiation 1, a beam splitter 2, a first modulating device 3, a second modulating device 4, a polarisation analyser 5 and a detector array 6.

The modulating devices 3, 4 are preferably dynamic modulating devices. However, it is possible to replace one or both of the dynamic modulating devices with a fixed polarisation-modulating device.

Electromagnetic radiation is emitted from the source of electromagnetic radiation 1 onto the beam splitter 2. A part of the beam passes through the beam splitter 2 and the remaining part is reflected onto the first modulating device 3. The first modulating device 3 then modulates the received electromagnetic radiation and displays the information to be encrypted/decrypted. Next the modulated electromagnetic radiation is reflected back to the beam splitter 2, where a part of the beam is reflected and thus leaves the module, and the remaining part passes through the beam splitter 2 and is received by the second

modulating device 4. The second modulating device 4 then encrypts/decrypts the information by changing the spatial polarisation state of the electromagnetic radiation received. This may e.g. be done by modulating the ellipticity of the electromagnetic radiation, such as by modulating the linear polarisation state or the circularity.

That is, in the encryption case, the image containing the information to be encrypted is "scrambled". In the decryption case the original information is retrieved from the scrambled image by applying an operation which is reverse to the operation being applied when the information was encrypted.

The electromagnetic radiation is then reflected back to the beam splitter 2, where a part of the beam passes through the beam splitter 2 and the remaining part is reflected onto the detector array 6, passing a polarisation analyser 5. The detector array 6 thus images the encrypted/decrypted information. Thus, an imaging operation takes place within the marked area 7.

The source of electromagnetic radiation 1 and the first modulating device 3 may be integrated, such that an array of emitting devices (matched in number and spatial location to the detector array 6 and second modulating device 4) which can independently have their polarisation state modulated may be used, thus effectively producing a hybrid device.

Fig. 2 shows a generic transmission geometry set-up. The operation of the module is very similar to what is outlined above in connection with Fig. 1. However, instead of reflective optical devices transmissive optical devices are used. That is, the electromagnetic radiation which has been emitted from the source of electromagnetic radiation 1 is transmitted through the first 3 and second 4 modulating devices rather than being reflected from them. Imaging operations take place within the two marked areas 7.

The imaging operation between the first 3 and second 4 modulating devices may involve the use of optical components, such as one or more lenses, or, if the components are close together, a free space propagation of the radiation between the aligned local elements on the modulating device 3, 4 may be possible. If the components are close together, such as immediately adjacent to each other, the overall dimensions of the module are reduced to a minimum limited by the dimensions of the individual components.

A combined emitter and modulator module could also be used to replace the source of electromagnetic radiation 1 and the first modulating device 3 as described above in connection with Fig.1.

Fig. 3 shows a preferred embodiment of a polarisation encryption/decryption module based on a single lens in a 2f optical configuration, f being the focal length of optical lens 8. The set-up is similar to the generic reflection geometry set-up shown in Fig. 1. Thus, the module comprises a source of electromagnetic radiation 1, a beam splitter 2, a first modulating device 3, a second modulating device 4, a polarisation analyser 5 and a detector array 6 as has already been described above. The module further comprises an optical lens 8 and a half wave plate 9.

In this preferred embodiment of the high-speed dynamic encryption and decryption system, the first 3 and second 4 modulating devices operate in reflection geometry receiving an input wavefront and modulating this locally by a rotation of the polarisation vector of the incident electromagnetic radiation. The electromagnetic radiation emitted by the source of electromagnetic radiation 1 may be inherently polarised as is the case with a diode laser or a polarising element (not shown) may be present to select the required direction of linear polarisation at the input. The polarised input radiation is incident on a transparent optical device 2 capable of splitting a portion of the beam away from the original propagation direction (a beam splitter). This split off beam is normally incident on the active region of the first modulating device 3, which spatially modulates the polarisation of the beam and reflects the modulated light along the input path for the split off beam. This beam passes through the beam splitter 2 and a portion of the light is transmitted directly through the beam splitter 2 whilst another not necessarily equal portion is reflected back onto the path of the input light where it is effectively lost from the system. The transmitted portion of the beam passes through a single lens 8, which performs an imaging operation between the active regions of the two modulating devices 3, 4. Thus the polarisation state of the wavefront reflected from the first modulating device 3 is imaged onto the second modulating device 4 where it is again modulated with a different spatial variation of the polarisation state so as to act on the information that has been encoded on the electromagnetic radiation by the first modulating device 3. The wavefront that is reflected from the second modulating device 4 is thus encrypted/decrypted and this must now be imaged onto a detector array 6 to determine

the information encoded in the polarisation. This imaging operation uses the afore mentioned single lens 8 and beam splitting device 2 to image the information from the second modulating device 4 onto the detector array 6 which is placed in an image plane which is equivalent to that in which the first modulating device 3 is placed. Thus the separation between the important system image planes (the distance between the first 3 and second 4 modulating devices) and (the distance between the second modulating device 4 and the detector array 6) are the same and correspond to a distance which is four times the focal length (f) of the afore mentioned lens 8. The lens 8 is therefore a distance of twice the focal length from the three image planes mentioned.

In the preferred embodiment is positioned a half wavelength thickness birefringent plate 9 which acts to flip the linear polarisation axes of the spatially polarisation encoded wavefronts about the fast axis of the birefringent half wavelength thickness plate 9. This improves the readout performance of the detector array 6 in the preferred embodiment. In order to convert the polarisation modulation in the encrypted/decrypted wavefront into an intensity modulation, which can be recorded on a detector array 6, a polarisation analyser 5 is placed in front of the detector array 6. This polarisation analyser 5 has its transmission axis oriented orthogonally to the linear polarisation axis of the input electromagnetic radiation. This ensures that direct transmission of input radiation through the beam splitting device 2 and onto the detector array 6 is prevented.

Fig. 4A shows a schematic representation of an encryption method and Fig. 4B shows a schematic representation of a decryption method according to the invention.

The components required for each process are identical and comprises a pair of modulating devices 3, 4 aligned such that the two fast axes corresponding to their binary states are parallel. These modulating devices 3, 4 are placed between a pair of polarisors 5 with a detector array 6 at the output to convert the optical signal to a digital signal. The encryption/decryption is performed by a direct pixel-to-pixel mapping of the original information to be transmitted with an encrypting/decrypting key.

In the example shown in Fig. 4A, the original information by a 7x7 pixel array, which contains a simple "smiling face" character, is represented at the first modulating device 3. This information is imaged onto a random encrypting key (at the second modulating device 4), which scrambles the original information, generating a wavefront on which the

encrypted information resides as a spatial variation in the polarisation direction of the light. This polarisation variation can then be visualised as an intensity distribution on a detector array 6 by the placement of a polarisor 5 parallel to the input polarisation orientation. The original information is thus transferred from electronic to optical format by the first modulating device 3, it is then encrypted optically by the second modulating device 4. The detector array 6 reconverts the encrypted optical information back to electronic format, which can then be securely transmitted. The encrypted information detected by the detector array 6 is represented by a 7x7 pixel array with no recognisable features.

At the receiving end of the network the decryption system, Fig. 4B, repeats the electronic to optical conversion and applies the decrypting key (at the second modulating device 4) to recover the original information, which is reconverted into an electronic signal by the detector array 6. The fact that the original information is retrieved at the detector array 6 is represented by a 7x7 pixel array showing the "smiling face" which was the information being encrypted in Fig. 4A.

In short, the information encryption and decryption is undertaken in the optical domain and the transmission of the encrypted data takes place across a standard network in the electrical domain. For optimal performance, we would require a high data content per frame and a high frame rate to approach the data transmission speeds required for a practical system. An important advantage of this approach is its inherent flexibility, since it is possible to change the key as often as required during the transmission of a given stream of data, up to the limit where each individual data frame displayed on the first modulating device 3 is encrypted and decrypted by a different key displayed on the second modulating device 4.

In practice the first of the polarisers 5 selects a certain polarisation of the light. The first 3 as well as the second 4 modulating device then rotates the orientation $\pm 45°$ according to preselected criteria. That is, when the light leaves the second modulating device 4 the orientation of the polarisation has been rotated $+90°$, $-90°$ or it has maintained the original orientation.

The fact that the components are identical in the two cases is very important since this allows a module to be used for encryption as well as decryption. One module is therefore sufficient even if the user wishes to perform encryption as well as decryption.

Fig. 5 shows a schematic view of the encryption, transmission and decryption of a sequence of images. The images are encrypted in a first computer 10 and transmitted to a second computer 11 in which they are decrypted. The first computer 10 as well as the second computer 11 comprise an encryption/decryption module as described above. The two modules are identical, so that they are capable of encrypting as well as decrypting information. It would therefore be possible to perform a "reverse" operation, i.e. the second computer 11 encrypting images being transmitted to the first computer 10 in which they are decrypted. Thus, an actual communication may be performed between the two computers 10, 11.

In the situation shown in Fig. 5, data is considered in the form of the frame sequence A1, B2, C3 etc. which is encrypted by a key sequence Key1, Key2, Key3 etc. in an optical XOR operation to generate an encrypted random output sequence which is then transmitted electronically over a network from a first computer 10 to a second computer 11. When the information has been encrypted in the first computer 10 it is recorded on a detector array 6 such as a CCD camera where it is converted into an encrypted digital signal suitable for transmission. At the receiving end (the second computer 11) the random output sequence serves as the input to be displayed on the first modulating device 3 of the decryption system and the required key sequence Key1, Key2, Key3 is applied, and an XOR operation recovers the original frame sequence A1, B2, C3. That is, the signal undergoes the reverse process to retrieve the original information. In short, the key can be different for each frame and it is the same size as the number of pixels in an individual frame. The use of an XOR operation ensures that the same system can both encrypt and decrypt information. Thus using a 256x256 pixel FLC-SLM and encoding a single bit of information per pixel, the effective key length would be 65,536 bits and the corresponding number of key combinations would be two raised to the power of this effective key length.

The key used for decrypting an encrypted image is most preferably the complex conjugate of the key used to encrypt the image. In special cases the same key can be applied for the two operations.

The advantage of the dual modulator approach as described above is that the key can be changed regularly for example on a frame-by-frame basis. In short the information

encryption and decryption is undertaken in the optical domain and the transmission of the encrypted information takes place across a standard network in the electrical domain. For optimal performance, we would require a high data content per frame and a high frame rate to approach the transmission speeds required for a practical data transmission network. Commercially available ferro-electric liquid crystal spatial light modulators (FLC-SLMs) offer a realistic possibility of meeting the data transmission rates for such a demanding application. Thus, binary 256x256 pixel FLC-SLMs (Displaytech) can be operated at frame rates of up to 2.5 kHz. By encoding the SLM so that one pixel displays a single bit a theoretical data transmission limit of 164 Mbs^{-1} is approached. The encrypted key length would then be 65 kb, which is extremely attractive in terms of both the encryption level and the data rate.

Experimental details

An experimental system has been constructed to test the polarisation encoding approach using ferro-electric liquid crystal SLMs. We have used a pair of 256x256 pixel FLC-SLMs (Displaytech Inc.) with a pixel pitch of 15 μm and a fill factor of 87 %. The devices operate in a reflection mode, which results in the experimental geometry shown in Fig. 6. The light source is a 635 nm laser diode (Hitachi HL6316G) operated in a multiple transverse mode regime since this reduces the deleterious effects of speckle on the image quality at the output which is observed when operating with a high spectral purity laser line. The laser is spatially filtered to produce a collimated beam, which is incident on SLM1 through a non-polarising cube beam splitter (BS). The two SLMs are imaged onto one another using a 4-f set-up (where L1 and L2 are achromatic doublets with f=7.5 cm). The 633 nm half-waveplate (λ/2) is used to compensate for the wavelength difference between that of the laser and that at which the SLM is designed to operate as a half-waveplate (680 nm in the case of the Displaytech FLC-SLM). Rotating this waveplate can dramatically improve the contrast of the output image.

Operation of the system

The SLMs are aligned for a direct pixel-to-pixel XOR operation between the input image plane (SLM1) and the key image plane (SLM2). The encrypted/decrypted information is subsequently imaged back through the same 4-f set-up and via the beam splitter through a polarisor oriented orthogonally with respect to the polarisation plane of the input laser light. A detector array with a pixel spacing matching that of the SLMs could then be placed in the output image plane (I) for a direct imaging of the result from the XOR operation.

However a mismatch between the SLM pixel pitch and that of the detector array will result in a sampling problem in the output image when camera pixels receive light from more than one SLM pixel.

In this demonstration system we have used a standard 1/3" CCD camera (Hitachi KP-M3E), which has a pixel pitch of 6.5 μm and 6.25 μm in the horizontal and vertical directions, respectively. It is apparent that attempting a 1:1 imaging operation between SLM2 and this CCD will result in a significant number of camera pixels integrating the signal from adjacent pixels and the dead space in between them. We have therefore chosen to use additional optics to improve the imaging of the output information. A second 4-f set-up (L3 and L4) has thus been used to magnify the output image by a factor of three.

Experimental Results

In Fig. 7, we show the test patterns that have been used for the encryption and decryption experiments. The information shown takes the form of a simple 256x256-pixel binary bitmap using one SLM pixel to represent one data pixel. A decryption operation is simply an XOR operation between the encrypted information Fig. 7(a) and the key shown in Fig. 7(b). The result of this decryption operation is the retrieval of the encrypted information as shown in Fig. 7(c).

In this case, we have chosen a test image, which contains a wide range of large and small-scale features so that a simple visual interpretation of the output data can determine alignment accuracy and the success of the decryption. In a real system however, a frame would simply be a pattern corresponding to the original electronic data stream we wished to encrypt or decrypt.

In Fig. 8(a), we show an experimental result from the decryption operation that is shown schematically in Fig. 7. Comparing Fig. 8(a), with the original information shown in Fig. 7(c) we can see that the decryption is successful with most features clearly reconstructed.

However there is some noise and non-uniformity in the decrypted image, which we believe is associated primarily with the imaging system, particularly the mismatch between the CCD and SLM pixel pitch and non-uniformities in the collimated laser beam profile. This becomes apparent when we examine the imaging properties of the optical

system directly as shown in Fig. 8(b). Here the unencrypted information given in Fig. 7(c) is displayed on SLM1 and imaged through the optical system with SLM2 acting passively as a mirror. In addition, due the magnifying imaging system (lenses L3 and L4 in Fig. 6), the images shown in Fig. 8 are composites of 16 individual CCD camera images laterally shifted with respect to one another in the output imaging plane. A certain amount of contrast variation thus appears to have been introduced by the automatic gain control of the CCD chip.

Operating the current system at a 3 kHz frame rate would result in a theoretical encrypted data transfer rate of approximately 200 Mbit/s with a 2^{16}-bit key length. This compares favourably with current electronic hardware encryption systems where rates of up to 180 Mbit/s can be achieved depending on the encryption algorithms and key length being used

An encrypted data rate in excess of 1 Gbit/s could be reached using an optical approach by doubling the SLM side length and increasing the frame rate to around 4 kHz, both of which are well within the technical limitations of the technology.

Thus, a polarisation encryption/decryption module has been provided which is compact in size and fast and which is being capable of performing encryption as well as decryption. This is obtained by using optical encryption/decryption and by using changing of the spatial polarisation state of the electromagnetic radiation, this providing a very fast operation.

CLAIMS

1. A polarisation encryption/decryption module comprising

- at least two array based modulating devices,
- at least one array based intensity detecting device,
- at least one source of electromagnetic radiation,

the at least two array based modulating devices having substantially the same functionality,

the at least one source(s) of electromagnetic radiation being capable of emitting electromagnetic radiation,

a first of the array based modulating devices being capable of receiving and modulating electromagnetic radiation which has been emitted from the at least one source(s) of electromagnetic radiation and of displaying information to be encrypted/decrypted,

a second of the array based modulating devices being capable of changing the spatial polarisation state of the electromagnetic radiation, so as to perform an operation of encrypting/decrypting the information displayed at said first array based modulating device,

wherein a local region of information displayed on said first array based modulating device has corresponding local regions on each of the other of the at least two array based modulating devices and on each of the at least one array based intensity detecting device(s).

2. A polarisation encryption/decryption module according to claim 1, wherein at least one of the at least two array based modulating devices is a dynamic array based modulating device.

3. A polarisation encryption/decryption module according to claim 1 or 2, wherein at least one of the at least two array based modulating devices is a fixed array based modulating device.

4. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is a reflective optical device.

5. A polarisation encryption/decryption module according to claim 4, wherein at least one of the at least two array based modulating devices is a reconfigurable spatial light modulator (SLM).

6. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is a transmissive optical device.

7. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least one electromagnetic source(s) is incorporated in one of the at least two array based modulating devices.

8. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is capable of modulating the ellipticity of the electromagnetic radiation.

9. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is capable of modulating the linear polarisation state of the electromagnetic radiation.

10. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is capable of modulating the circularity of the polarisation of the electromagnetic radiation.

11. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is a ferro-electric liquid crystal spatial light modulator (FLC-SLM).

12. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is based on a birefringent material or effect.

13. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is based on an anisotropic refractive index effect.

14. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is a nematic liquid crystal spatial light modulator (SLM).

15. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least two array based modulating devices is based on arrays of polarising elements.

16. A polarisation encryption/decryption module according to any of the preceding claims, wherein the information to be encrypted/decrypted comprises at least one two-dimensional image.

17. A polarisation encryption/decryption module according to any of the preceding claims, wherein the information to be encrypted/decrypted comprises at least one one-dimensional array of information.

18. A polarisation encryption/decryption module according to any of the preceding claims, wherein the outer dimensions of the module do not exceed 100 mm x 100 mm x 100 mm.

19. A polarisation encryption/decryption module according to claim 18, wherein the outer dimensions of the module do not exceed 80 mm x 80 mm x 50 mm.

20. A polarisation encryption/decryption module according to claim 19, wherein the outer dimensions of the module do not exceed 75 mm x 75 mm x 30 mm.

21. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least one source(s) of electromagnetic radiation is capable

of emitting electromagnetic radiation within the optical frequency range of the electromagnetic spectrum.

22. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least one source(s) of electromagnetic radiation is a laser.

23. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least one array based intensity detecting device(s) is a charge coupled device (CCD) camera.

24. A polarisation encryption/decryption module according to any of the preceding claims, wherein at least one of the at least one array based intensity detecting device(s) is a dedicated complementary metal oxide semiconductor (CMOS) detector.

25. A method of polarisation encrypting/decrypting information using a module according to any of claims 1-24, the method comprising the steps of

a) at least one of the at least one source(s) of electromagnetic radiation emitting electromagnetic radiation,

b) a first of the at least two array based modulating devices receiving and modulating electromagnetic radiation which has been emitted from the at least one source(s) of electromagnetic radiation,

c) the first of the at least two array based modulating devices displaying the information to be encrypted/decrypted,

d) a second of the at least two array based modulating devices changing the spatial polarisation of the electromagnetic radiation, thereby performing an operation of encrypting/decrypting the information displayed at said first array based modulating device,

e) at least one of the at least one array based intensity detecting device(s) detecting the result of the encryption/decryption process performed by said second array based modulating device,

the encryption/decryption being performed in such a way that a local region of information displayed on said first array based modulating device has corresponding local regions on each of the other of the at least two array based modulating devices and on each of the at least one array based intensity detecting device(s).

26. A method according to claim 25, wherein the steps a)-e) are performed two or more times.

27. A method according to claim 25 or 26, at least one of the at least one source(s) of electromagnetic radiation being incorporated in one of the at least two array based modulating devices, wherein step a) comprises emitting electromagnetic radiation via the one of the at least two array based modulating devices having the electromagnetic source(s) incorporated in it.

28. A method according to any of claims 25-27, wherein step d) is performed by modulating the ellipticity of the electromagnetic radiation.

29. A method according to any of claims 25-27, wherein step d) is performed by modulating the linear polarisation state of the electromagnetic radiation.

30. A method according to any of claims 25-27, wherein step d) is performed by modulating the circularity of the electromagnetic radiation.

31. A method according to any of claims 25-30, the information to be encrypted/decrypted comprising two or more successive two-dimensional images, wherein the steps a)-e) are performed at least once for each two-dimensional image, and wherein step d) is performed in a way which is different for each image, so that a sequence of encrypted/decrypted images is produced.

32. A method of polarisation encrypting and decrypting information using at least two polarisation encryption/decryption modules according to any of claims 1-24, the method comprising the steps of

- a first of the at least two polarisation encryption/decryption modules encrypting the information using a method according to any of claims 25-31,
- transmitting the encrypted information from said first polarisation encryption/decryption module to a second of said at least two polarisation encryption/decryption modules,
- said second polarisation encryption/decryption module decrypting the information using a method according to any of claims 25-31.

33. A method according to claim 32, wherein at least the transmitting step is performed using at least one computer device.

34. A method according to claim 32 or 33, the method being performed using a plurality of polarisation encryption/decryption modules according to any of claims 1-24, the method further comprising the steps of

- transmitting the encrypted information from said first polarisation encryption/decryption module to at least a third of said plurality of polarisation encryption/decryption modules,
- each of said at least third polarisation encryption/decryption module(s) decrypting the information using a method according to any of claims 25-31.

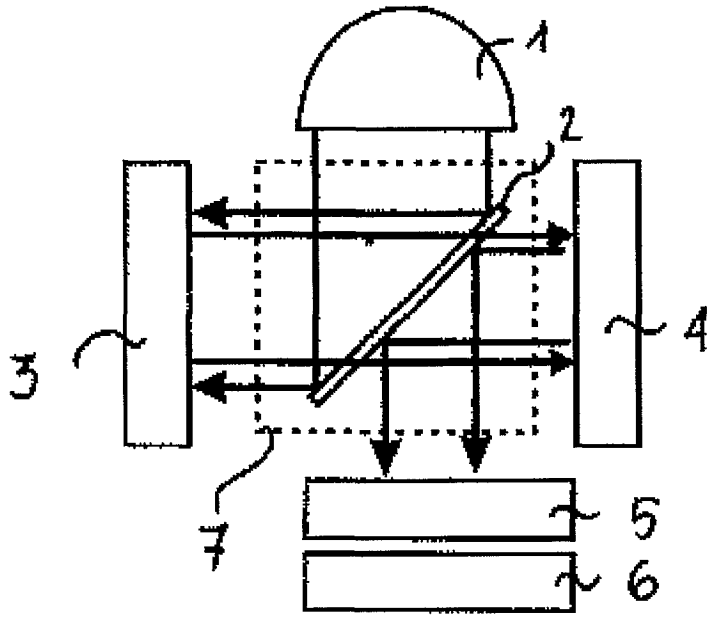


Fig. 1

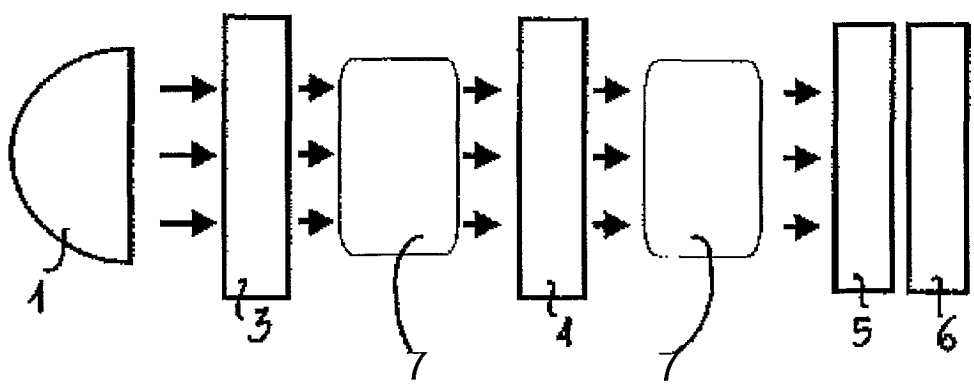


Fig. 2

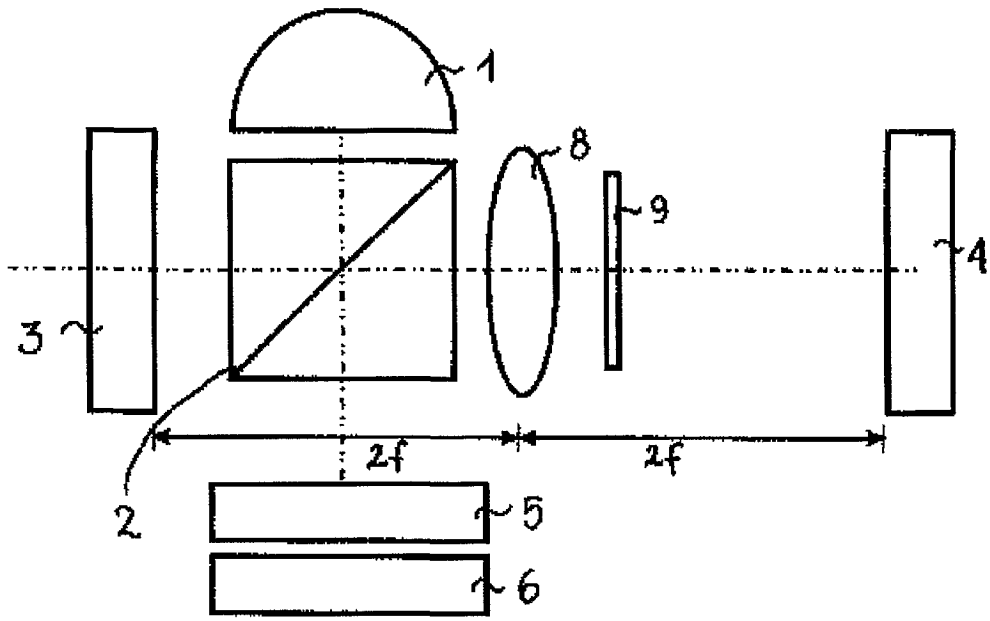

1
8
9
4
3
2f
2f
2
5
6

Fig. 3

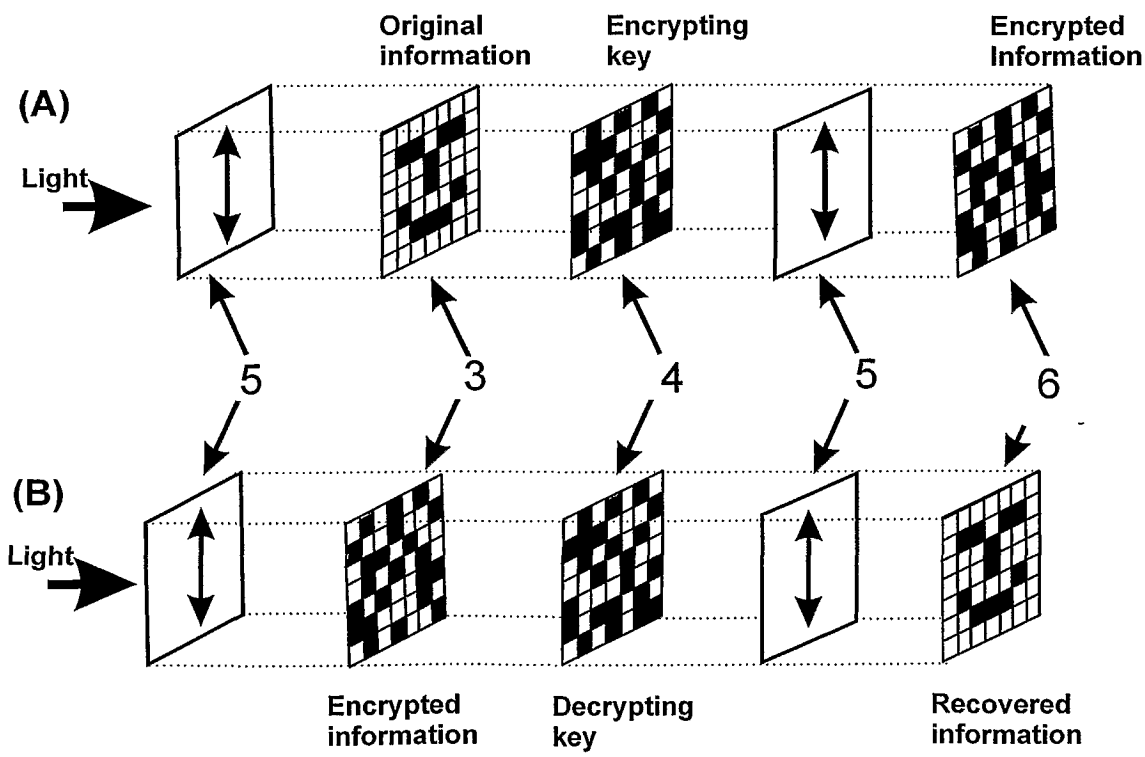

Original information
Encrypting key
Encrypted Information
(A)
Light
5
3
4
5
6
(B)
Light
Encrypted information
Decrypting key
Recovered information

Fig. 4

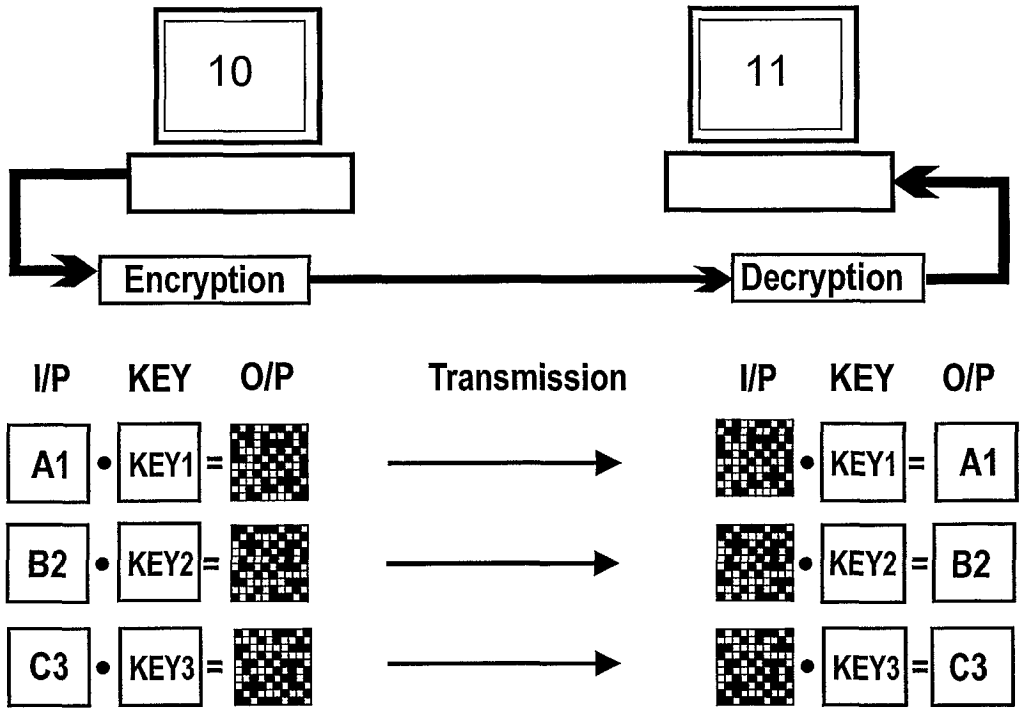

10
11
Encryption
Decryption
I/P
KEY
O/P
Transmission
I/P
KEY
O/P
A1
KEY1
A1
B2
KEY2
B2
C3
KEY3
C3

Fig. 5

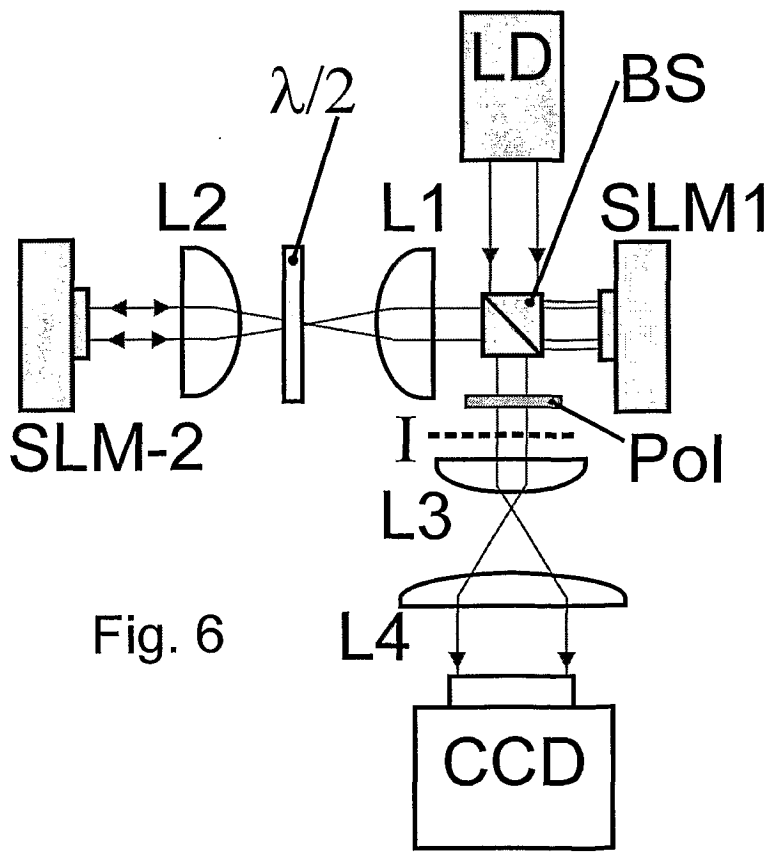

LD
BS
λ/2
L2
L1
SLM1
SLM-2
I
Pol
L3
L4
CCD

Fig. 6

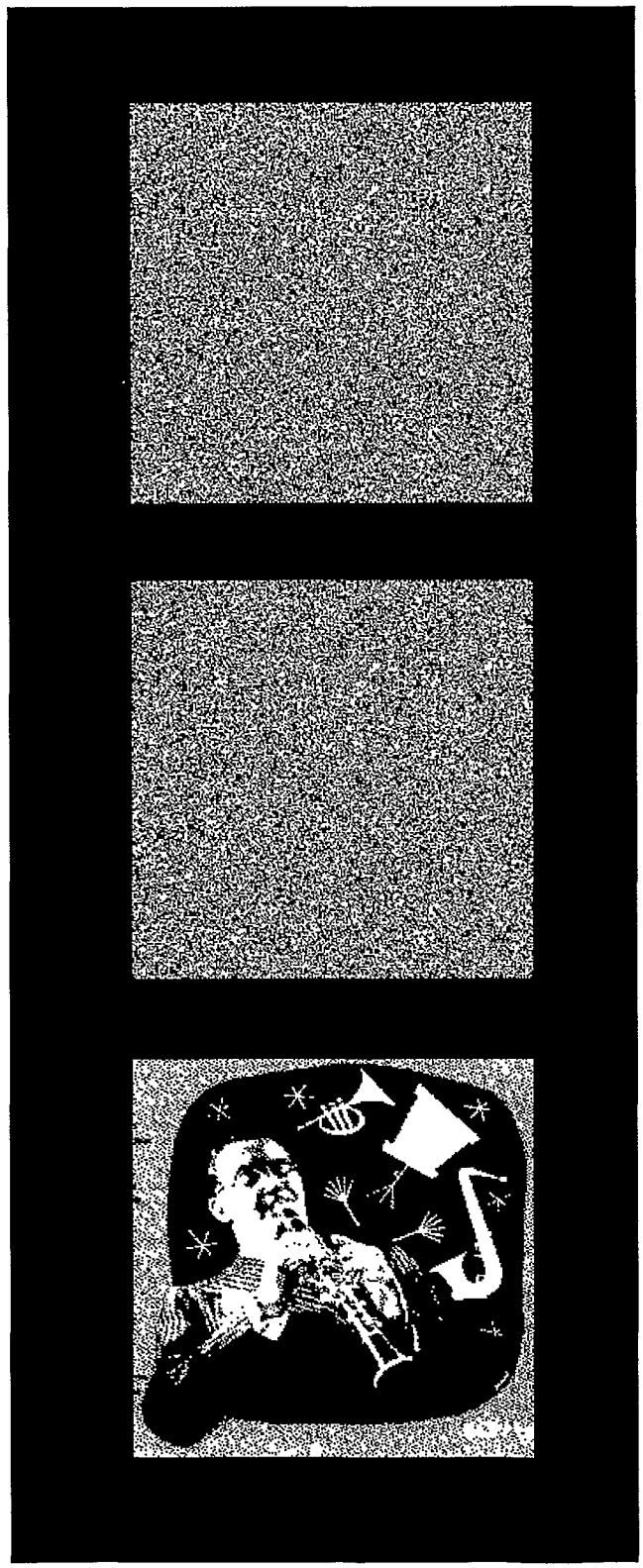


Fig. 7A

Fig. 7B

Fig. 7C

Fig. 8A

Fig. 8B